United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ALICE SVENSON, individually and on behalf of all others similarly situated,

Plaintiff,

v.

GOOGLE INC., a Delaware Corporation, and GOOGLE PAYMENT CORPORATION, a Delaware Corporation,

Defendants.

Case No. 13-cv-04080-BLF

ORDER DENYING MOTION TO DISMISS FOR LACK OF ARTICLE III STANDING; AND GRANTING MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM WITH LEAVE TO AMEND IN PART

[Re: ECF 20]

In this putative class action, Plaintiff Alice Svenson alleges that Defendants Google Inc. and Google Payment Corporation make unauthorized disclosures of user information to third-party developers of mobile applications ("Apps") when users purchase Apps in the Google Play store using Google Wallet. Defendants move to dismiss under Federal Rule of Civil Procedure 12(b)(1) for lack of Article III standing and under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim. The Court has considered the briefing and the oral argument presented at the hearing on June 26, 2014. For the reasons discussed below, the motion to dismiss for lack of Article III standing is DENIED and the motion to dismiss for failure to state a claim is GRANTED with leave to amend in part.

I. BACKGROUND

Plaintiff alleges that "Google provides internet search functionality, email services, virtual filing cabinet 'cloud' storage services, multimedia electronic distribution platforms, social media services, advertising services, and payment processing services, among many others." (Corrected Complaint ("Compl.") ¶ 10, ECF 5-1) Google Wallet is "Google's electronic and mobile payment

processing service." (*Id.* ¶ 17) Google Wallet allows users to store debit card and credit card information and to utilize those payment methods to purchase Apps and other products. (*Id.* ¶¶ 17-18) Apps may be purchased in the Google Play store, "Google's digital multimedia content distribution platform that is accessible via mobile devices and other internet-capable computing equipment." (*Id.* ¶¶ 26, 28)

When a user purchases an App in the Google Play store using Google Wallet, "Defendants process the payment." (Compl. ¶ 49) "After Defendants process the user's payment, Defendants automatically remit funds to the third-party vendor in addition to the user's name, email address, Google account name, home city and state, zip code, and in some instances telephone number" (hereinafter, "Contact Information").[1] (*Id.*) Google transmits the App to the user electronically via the Google Play store. (*Id.* ¶ 47)

The Contact Information is collected by Defendants when users register for a Google account, Gmail, the Google Play store, or Google Wallet. (Compl. ¶ 55) Plaintiff asserts that disclosure of Contact Information to third-party vendors is unnecessary and unauthorized by the user (*id.* ¶¶ 50-51, 54); breaches the terms of the agreements between the users and Defendants (*id.* ¶¶ 65-66); diminishes the economic value of the Contact Information (*id.* ¶¶ 83-84); and exposes the user to a greater risk of identity theft (*id.* ¶ 89).

Plaintiff alleges that on May 6, 2013, she bought an App in the Google Play store using Google Wallet. (Compl. ¶ 74). Specifically, Plaintiff paid $1.77 for the "SMS MMS to Email" App published by third-party vendor YCDroid; upon purchase, the App was instantly downloaded for use on Plaintiff's mobile device. (*Id.*) Following the purchase, Defendants "transmitted and/or made available" Plaintiff's Contact Information to YCDroid. (*Id.* ¶ 77) Based upon this transaction, Plaintiff asserts claims against Defendants for: (1) breach of contract; (2) breach of the implied covenant of good faith and fair dealing; (3) violation of the Stored Communications

[1] Plaintiff's complaint and briefs use the term "Sensitive Identifiable Data," abbreviated to "SID" to describe this information, while Defendants' briefs use the term "Contact Information." Because the term "Contact Information" is less unwieldy than the term "Sensitive Identifiable Data" and accurately describes the information, the Court uses the term "Contact Information" in this order.

Act, 18 U.S.C. § 2701; (4) violation of the Stored Communications Act, 18 U.S.C. § 2702; and (5) violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200.

Defendants contend that Plaintiff has failed to allege facts demonstrating that she has Article III standing and thus has failed to establish subject matter jurisdiction. Alternatively, Defendants contend that Plaintiff has failed to allege facts sufficient to state a claim upon which relief may be granted.

II. LEGAL STANDARDS

A. Rule 12(b)(1)

A motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(1) raises a challenge to the Court's subject matter jurisdiction. *See* Fed. R. Civ. P. 12(b)(1). "Article III . . . gives the federal courts jurisdiction over only cases and controversies." *Public Lands for the People, Inc. v. United States Dep't of Agric.*, 697 F.3d 1192, 1195 (9th Cir. 2012) (internal quotation marks and citation omitted). "The oft-cited *Lujan v. Defenders of Wildlife* case states the three requirements for Article III standing: (1) an injury in fact that (2) is fairly traceable to the challenged conduct and (3) has some likelihood of redressability." *Id.* at 1195-96 (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). If these requirements are not satisfied, the action should be dismissed for lack of subject matter jurisdiction. *See Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 109-10 (1998).

B. Rule 12(b)(6)

"A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted 'tests the legal sufficiency of a claim.'" *Conservation Force v. Salazar*, 646 F.3d 1240, 1241-42 (9th Cir. 2011) (quoting *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001)). When determining whether a claim has been stated, the Court accepts as true all well-pled factual allegations and construes them in the light most favorable to the plaintiff. *Reese v. BP Exploration (Alaska) Inc.*, 643 F.3d 681, 690 (9th Cir. 2011). However, the Court need not "accept as true allegations that contradict matters properly subject to judicial notice" or "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008)

(internal quotation marks and citations omitted). While a complaint need not contain detailed factual allegations, it "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible when it "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.*

III. DISCUSSION

A. Subject Matter Jurisdiction

In their motion, Defendants argue that Plaintiff has not alleged facts sufficient to establish Article III standing and thus that the Court lacks subject matter jurisdiction. After Defendants filed the motion, the Ninth Circuit clarified that a plaintiff suing under the Stored Communications Act ("SCA") has Article III standing. *See In re Zynga Privacy Litig.*, 750 F.3d 1098, 1105 n.5 (9th Cir. 2014). In that case, Defendants Zynga and Facebook argued that the plaintiffs lacked standing to assert claims under the Wiretap Act and the SCA because they had "not suffered any concrete or particularized injury arising from the alleged disclosure of users' Facebook IDs and URL information to third parties." *Id.* The court rejected that argument, holding that "a plaintiff demonstrates an injury sufficient to satisfy Article III when bringing a claim under a statute that prohibits the defendant's conduct and grants persons in the plaintiff's position a right to judicial relief." *Id.* (internal quotation marks and citation omitted). The Court held that because the plaintiffs alleged that Zynga and Facebook were violating the Wiretap Act and the SCA – statutes granting persons in the plaintiffs' position the right to judicial relief – they had standing to proceed. *Id.* Defendants in the present case concede that *Zynga* resolves the Article III standing issue for purposes of this motion. (Defs.' Supp. Br. at 1, ECF 74)

Accordingly, the motion to dismiss for lack of Article III standing is DENIED.

B. Failure to State a Claim

1. Claim 1 – Breach of Contract

Claim 1 alleges breach of contract. To succeed on a breach of contract claim under California law, a plaintiff must establish a contract, the plaintiff's performance or excuse for nonperformance, the defendant's breach, and resulting damages to the plaintiff. *Pyramid Tech.*,

Inc. v. Hartford Cas. Ins. Co., 752 F.3d 807, 818 (9th Cir. 2014).

a. Relevant Contracts

Plaintiff alleges the existence of a number of agreements that governed her App purchase: the Google Terms of Service ("GToS") (Compl. ¶ 20); the Google Privacy Policy ("GPP") (*id.*); the Google Wallet Terms of Service ("GWToS") (*id.* ¶ 21); the Google Wallet Privacy Policy ("GWPP") (*id.*); and the Google Play Terms of Service ("GPToS") (*id.* ¶ 27). Plaintiff does not attach any of these agreements to her complaint.

As is discussed below, Plaintiff's failure to attach the agreements as exhibits to the complaint, and her decision instead to include hyperlinks in the text of the complaint (some of which were inaccurate), needlessly multiplied and confused the proceedings. While Plaintiff is not required to do so, the Court strongly urges Plaintiff to attach the relevant contracts to any amended complaints she may file in this case.

Defendants request judicial notice of the GWToS and the GWPP. (Defs.' RJN, ECF 21) Plaintiff objects to Defendants' request, arguing that Defendants have submitted the September 10, 2013 GWToS when Plaintiffs' claims are governed by the October 23, 2012 GWToS. Plaintiff submits the October 23, 2012 GWToS in connection with her own request for judicial notice. (Pl.'s RJN, ECF 31, 36) Defendants do not object to the Court's consideration of the October 23, 2012 GWToS, as Defendants state that there is no material difference between the two versions of the GWToS; Defendants explain that they submitted the later GWToS only because the complaint referenced a link to that version. (Defs' Resp. to Pl.'s Objs., ECF 52) Defendants likewise do not object to Plaintiff's request for judicial notice of Proposition 64, the relevant GPToS, and the relevant GToS. Judicial notice is appropriate with respect to Proposition 64. *See Kamen v. Kemper Fin. Svcs., Inc.*, 500 U.S. 90, 99 (1991) (courts may take judicial notice of the law of any state). The GWPP submitted by Defendants and the GPToS, GWToS, and GToS submitted by Plaintiff may be considered under the incorporation by reference doctrine. *See Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005) (the incorporation by reference doctrine permits a court to consider documents referenced in but not physically attached to the complaint).

b. Allegations of Breach

Plaintiff claims that "the GWPP and GPP, as incorporated into the GWToS, constitute a valid and enforceable contract between Plaintiff and the Class and Defendants." (Compl. ¶ 102). Plaintiff alleges generally that under this contract, "Plaintiff and the Class agreed to register with the Google Play store and Google Wallet to allow Defendants to process their purchase and payment transactions in connection with provision and sale of Apps." (*Id.* ¶ 100) According to Plaintiff, "[t]hese transactions thereby allow Google Payment Corp to earn a fee for processing the payment." (*Id.*) In exchange, Defendants acted as "a middle-man" in the App transactions, and they agreed to share users' Contact Information with third parties only in specific, limited circumstances. (*Id.* ¶¶ 103-06) Plaintiff alleges that she "and the Class did all or substantially all of the significant things required of them by the Relevant Terms." (*Id.* ¶ 107) She alleges that Defendants breached the contract by sharing her Contact Information under circumstances not contemplated by the agreements. (*Id.* ¶¶ 103-06) Finally, she alleges that "Plaintiff and the Class are damaged and are alternatively entitled to restitution for Defendant's unjust enrichment due to Defendants' aforesaid breaches." (*Id.* ¶ 108)

These allegations are insufficient to state a claim for breach of contract. Initially, Plaintiffs' identification of the "contract" is inadequate. While Plaintiff alleges that the "contract" is a combination of the GWPP, GPP, and GWToS (Compl. ¶ 102), Plaintiff has admittedly identified the wrong contracts in her complaint.

More significantly, Plaintiff's conclusory allegation that she and the Class "are damaged" is insufficient to plead this element of her contract claim. *See Iqbal*, 556 U.S. at 678 ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice."). Additionally, Plaintiff's alternative allegation that she and the Class are entitled to restitution as a result of Defendants' breach of contract is simply incorrect as a matter of law. Generally, if two parties have a valid and enforceable written contract, the plaintiff may not proceed on a claim in quasi-contract, *i.e.*, a claim of restitution or unjust enrichment. *See Klein v. Chevron U.S.C., Inc.*, 202 Cal. App. 4th 1342, 1388 (2012). "[A] plaintiff may not plead the existence of an enforceable contract and maintain a quasi-contract claim at the same time, unless

the plaintiff has pled facts suggesting that the contract may be unenforceable or invalid." *Schulz v. Cisco Webex, LLC*, No. 13-cv-04987-BLF, 2014 WL 2115168, at *5 (N.D. Cal. May 20, 2014).

Plaintiff's allegations of breach of contract and resulting damages are set forth in paragraphs 74-89 and 98-108 of the complaint. In essence, Plaintiff alleges that upon purchase of the App, Google disclosed her Contact Information to the third-party App vendor but that disclosure was not "necessary" for the transaction with the third-party vendor and thus violated the privacy provisions of the various contracts at issue. (Compl. ¶ 106) Plaintiff alleges three theories of contract damages: benefit of the bargain, diminution in the economic and proprietary value of her Contact Information, and increased risk of identity theft.

With respect to her benefit of the bargain theory of damages, Plaintiff alleges that the $1.77 she paid for the App included "built-in monies and transaction fees pocketed by Defendant Google Payment Corp."; that those monies compensated Google for the "service" of facilitating the App purchase *without* disclosing Plaintiff's Contact Information; and that Plaintiff was denied the benefit of her bargain when Defendants "pocketed monies" from the App purchase but nonetheless transmitted Plaintiff's Contact Information to the third-party vendor when there was no necessity to do so. (Compl. ¶¶ 79-81)

Those allegations are insufficient because they do not show that Plaintiff paid anything for the asserted privacy protections. Plaintiff entered into the Google, Google Wallet and Google Play agreements separately from her actual purchase of the App. (Compl. ¶¶ 68-70, 74) She does not allege that she made any payment for those services. In fact, a review of the contracts makes it clear that those were all free services. (*See e.g.*, Pl.'s RJN Ex. 3 (GWToS) ("GPC does not charge a fee to use the Processing Service as a Buyer.") Plaintiff does not allege facts showing that she entered into a new or different agreement upon purchase of the App that could have given rise to new or additional privacy protections. It appears clear from the face of the complaint that the only payment made was the $1.77 to the third- party vendor for the App, and Plaintiff does not allege that any portion of that $1.77 was retained by Defendants rather than being transmitted in full to the vendor. Finally, even if Plaintiff's benefit of the bargain theory were not defective for the foregoing reasons, Plaintiff does not allege that what she received – the App and unauthorized

disclosure of her Contact Information – was worth less than what she allegedly bargained for – the App and non-disclosure of her Contact Information.

As to her second damages theory, Plaintiff alleges that the disclosure of her Contact Information to the third-party vendor diminished the economic and proprietary value of the Contact Information to her. (Compl. ¶ 82) A recent unpublished decision of the Ninth Circuit Court of Appeals suggests that this type of allegation may be sufficient to establish the element of damages for a breach of contract claim. *See In re Facebook Privacy Litigation*, --- Fed.Appx. ----, No. 12–15619, 2014 WL 1815489, at *1 (9th Cir. May 8, 2014). At the hearing, Defendants' counsel asserted that the plaintiffs in that case had alleged a market for the information in question. That fact is not apparent from the decision, although as a matter of common sense a theory of diminished economic value would depend on the existence of a market for the information. Plaintiff has not alleged a market for her Contact Information.

Finally, Plaintiff alleges that Defendants' disclosure of her Contact Information has increased her risk of identity theft. That allegation is too speculative to satisfy the pleading requirement of contract damages. *See Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 917-18 (N.D. Cal. 2009).

In summary, it appears that a Gmail account and a Google Wallet account are free; all of the contractual privacy provisions upon which Plaintiff relies are contained in agreements that were entered into in connection with creation of those free accounts; and Plaintiff did not agree to any additional terms or pay any additional consideration when she purchased the $1.77 App that forms the basis of this lawsuit. Under these circumstances, it is not clear how Plaintiff could amend her complaint to allege contract damages. However, because this motion is the first challenge to the complaint, Plaintiff will be afforded an opportunity to cure the defects noted herein.

Accordingly, Defendants' motion is GRANTED with leave to amend as to Claim 1.

2. Claim 2 – Breach of the Implied Covenant

Claim 2 alleges breach of the implied covenant of good faith and fair dealing. "'The implied promise [of good faith and fair dealing] requires each contracting party to refrain from

doing anything to injure the right of the other to receive the benefits of the agreement.'" *Avidity Partners, LLC v. State of Cal.*, 221 Cal. App. 4th 1180, 1204 (2013) (quoting *Egan v. Mutual of Omaha Ins. Co.*, 24 Cal. 3d 809, 818 (1979)). "The implied covenant of good faith and fair dealing does not impose substantive terms and conditions beyond those to which the parties actually agreed." *Id.*

Plaintiff alleges that Defendants' disclosure of her Contact Information ran contrary to her reasonable expectations and interfered with her right to receive the full benefit of the contract. (Compl. ¶ 114) This allegation is duplicative of Plaintiff's claim for breach of contract. When the allegations of a claim for breach of the implied covenant "do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a companion contract cause of action, they may be disregarded as superfluous as no additional claim is actually stated." *Careau & Co. v. Security Pacific Business Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990).

Plaintiff contends that there is no duplication of the contract claim in this case because the implied covenant claim includes additional allegations that "the Relevant Terms are standardized and non-negotiable terms, which Defendants, at their own discretion, interpreted to carry out the above-described privacy promises as they saw fit, in a way that resulted in transmission of Plaintiff and other Class members' [Contact Information] to third-party App vendors." (Compl. ¶ 112) While a claim for breach of the implied covenant may be made out by allegations that a defendant acted in bad faith to frustrate the agreed common purpose of the contract, *see Careau*, 222 Cal. App. 3d at 1395, the bad faith alleged on the part of Defendants here is simply breaching the contract by disclosing Plaintiff's Contact Information (*see* Compl. ¶ 114). Thus while Plaintiff may be able to flesh out this claim, as presently framed it is duplicative of her claim for breach of contract.

Defendants' motion is GRANTED with leave to amend as to Claim 2.

3. Claim 3 – Violation of SCA § 2701

Claims 3 and 4 assert that Defendants' disclosure of Plaintiff's Contact Information violated §§ 2701 and 2702 of the SCA, respectively. *See* 18 U.S.C. §§ 2701-02. "Enacted in

1986 as Section II of the Electronic Communications Protection Act ("ECPA"), the SCA creates criminal and civil liability for certain unauthorized access to stored communications and records." *In re iPhone Applic. Litig.*, 844 F. Supp. 2d 1040, 1056-57 (N.D. Cal. 2012); *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002) (discussing enactment of SCA).

Section 2701 of the SCA creates a private right of action against anyone who "(1) intentionally *accesses without authorization a facility* through which an electronic communication service is provided; or (2) intentionally *exceeds an authorization to access that facility*; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a) (emphasis added); *see id.* § 2707(a) (creating a private right of action). The prohibitions set forth in § 2701(a) do not apply "to conduct authorized – (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c).

Plaintiff alleges that Defendants utilize "server facilities," and that "[i]n the course of processing Plaintiff and the Class's Google Wallet App online purchases, Defendants exceeded their authorized access to the facilities through which Defendants provide the electronic communications services at issue and within which their [Contact Information] was stored on Defendants' servers, by unnecessarily transmitting or making available their [Contact Information] to third-party App vendors." (Compl. 119, 124) These allegations are insufficient to state a claim under section 2701(a). It appears from the face of the complaint that the "facility" in question was *Defendants' own servers*. (*See* Compl. ¶ 124, alleging that the Contact Information "was stored on Defendants' servers") Plaintiff does not allege any facts suggesting that Defendants were not authorized to access their own servers as required under § 2701(a). Likewise, it appears from the face of the complaint that *Defendants provide the electronic communications service at issue.* (*See id.* (alleging that "Defendants provide the electronic communications services at issue")) Plaintiff does not allege facts showing why Defendants thus would not be exempt from liability under § 2701(c). *See* 18 U.S.C. § 2701(c)(1) (exempting conduct authorized "by the person or entity providing a wire or electronic communications service").

Another court in this district confronted with a similar claim that Google had violated § 2701(a) held that:

> This claim borders on frivolous, considering the plain language of subsection (c) of Section 2701[] that exempts conduct authorized "by the person or entity providing a wire or electronic communications service." Whatever the propriety of Google's actions, it plainly authorized actions that it took itself.

In re Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *12 (N.D. Cal. Dec. 3, 2013) (footnote omitted). This Court agrees with the above analysis, and with other district courts that have dismissed § 2701(a) claims based upon the plaintiff's failure to allege unauthorized access to a "facility." *See, e.g., In re iPhone Applic. Litig.*, 844 F. Supp. 2d at 1057-58 (dismissing § 2701(a) claim after concluding that the iPhones allegedly accessed by the defendants were not "facilities" within the meaning of the statute).

At the hearing, Plaintiff's counsel argued that by sending Plaintiff's Contact Information to the third-party vendor, Defendants in essence granted the third-party vendor access to its servers (the "facility"). While Plaintiff raises an interesting question with respect to the meaning of "access" in the digital age, in order to make out a § 2701 claim against *Defendants*, Plaintiff must allege that *Defendants* engaged in unauthorized access of the facility. This they plainly cannot do here, as the facility in question belongs to Defendants.

Plaintiff argues that the line of cases discussed above applies §§ 2701(a) and (c) by rote, without giving sufficient consideration to whether a service provider should have blanket authority to access information on its servers. (*See* Opp. at 24, ECF 38) Regardless of the merits of Plaintiff's policy arguments, this Court is without authority to alter the plain language of the statute, which clearly does not apply to the facts alleged in the complaint. The cases relied upon by Plaintiff address different statutes or otherwise fail to support the statutory construction she urges here.

Accordingly, Defendants' motion is GRANTED without leave to amend as to Claim 3.

4. Claim 4 – Violation of SCA § 2702

Section 2702 of the SCA creates a private right of action for violation of the following provisions:

> (a) Prohibitions. – Except as provided in subsection (b) or (c) –
>
> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the *contents of a communication* while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the *contents of any communication* which is carried or maintained on that service –
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
>
> (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

18 U.S.C. § 2702(a) (emphasis added); *see id.* § 2707(a) (creating a private right of action).

While a provider described in subsection (a) may not disclose the "contents of a communication," such provider may divulge "*a record* or other information" regarding a subscriber or customer to "any person other than a governmental entity" and to governmental entities under certain circumstances. 18 U.S.C. § 2702(c) (emphasis added).

For purposes of this motion, Defendants do not dispute that Google is an entity "providing an electronic communication service" and/or "providing remote computing service" within the meaning of § 2702(a). (*See* Mot. at 17 n.10) The question presented by this motion is whether the Contact Information that Defendants sent to the third-party vendor was "contents of a communication" or "a record or other information"; if the former, Plaintiff has made out a claim under § 2702(a), but if the latter she has not. For the reasons discussed below, the Court concludes that the facts alleged in the complaint establish the disclosure of record information rather than contents of a communication.

"The 'contents' of a communication are 'any information concerning the substance, purport, or meaning of that communication." *Zynga*, 750 F.3d at 1105 (citing 18 U.S.C. §

2510(8)); *see also id.* at 1104 (noting that the SCA incorporates the Wiretap Act's definition of "contents"). The Ninth Circuit has explained that "the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *Id.* at 1106. The Ninth Circuit has recognized that record information generally includes "the name, address, or client ID number of the entity's customers." *Id.* at 1104.

In *Zynga*, the plaintiffs claimed that when users clicked on certain ads or icons on a Facebook webpage, the web browser sent a request to access the resource identified by the link and *also* sent a "referer header" comprising the user's Facebook ID and the address of the Facebook webpage the user was viewing when the user clicked the link. *Zynga*, 750 F.3d at 1101-02. The plaintiffs alleged that the referer header constituted contents of a communication such that its transmission to third parties violated § 2702(a). The Court held that the referer header did not meet the definition of "contents." *Id.* at 1107. Equating the Facebook ID with a user's "name" or "subscriber number or identity," and equating the webpage address with a user's "address," the Court held that "these pieces of information are not the 'substance, purport, or meaning' of a communication." *Id.*

The Court distinguished *In re Pharmatrak*, 329 F.3d 9 (1st Cir. 2003), a Wiretap Act case in which the defendants allegedly intercepted the contents of electronic communications, specifically, information that individuals provided to online pharmaceutical websites. That information included the individuals' "names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website." *Id.* at 15. It was undisputed that the information constituted "contents" of a communication under the circumstances of the case; the arguments focused on whether the "interception" element of the Wiretap Act claim was satisfied and whether the consent exception applied. *Id.* at 18. The Ninth Circuit opined in *Zynga* that the information in *Pharmatrak* properly was characterized as contents of a communication "[b]ecause the users had communicated with the website by *entering their personal medical information into a form provided by a website*." *Zynga*, 750 F.3d at 1107 (emphasis added). The Ninth Circuit

distinguished the case before it by noting that the *Zynga* defendants did not divulge a user's communications to a website but allegedly "divulged identification and address information contained in a referrer header automatically generated by the web browser." *Id.*

Although *Zynga* distinguished *Pharmatrak* in part on the basis that the referrer header at issue in *Zynga* was automatically generated, this Court does not read *Zynga* so narrowly to mean that *only* automatically generated data may constitute record information. The Contact Information at issue in the present case – the user's name, email address, Google account name, home city and state, zip code, and in some instances telephone number – is the type of information that the Ninth Circuit recognized as record information in *Zynga*. *See Zynga* at 1104 (recognizing that record information generally includes "the name, address, or client ID number of the entity's customers"). Numerous courts in this district likewise have characterized such information as record information in the context of civil discovery. *See, e.g. Chevron Corp. v. Donziger*, No. 12-mc-80237 CRB (NC), 2013 WL 4536808, at *6 (N.D. Cal. Aug. 22, 2013) (characterizing information associated with the creation of an email address, including names, mailing addresses, phone numbers, billing information, and date of account creation, as "record or other information" and not "contents" of a communication); *Obodai v. Indeed, Inc.*, No. 13-80027-MISC EMC (KAW), 2013 WL 1191267, at *3 (N.D. Cal. Mar. 21, 2013) (holding that no "content" of communications was implicated by a subpoena seeking "subscriber information" provided when a user creates a Gmail account, such as phone numbers and alternative email addresses). To hold that such information constitutes contents of a communication unless it was automatically generated would read § 2702(c) out of the statue.

Plaintiff relies heavily upon her assertion that the Contact Information was entered by means of a form interface such as that used in *Pharmatrak*, although that fact is not clear from the complaint. Even assuming Plaintiff's assertion to be true, the Court is not persuaded that the form interface was critical to the *Pharmatrak* decision. As noted above, it was undisputed in *Pharmatrak* that the information in question constituted contents of a communication. Indeed, any court would be hard-pressed to find that the highly personal disclosures in that case, which included insurance statuses, medical conditions, and medications, constituted mere record

information. The fact that the Ninth Circuit distinguished *Pharmatrak* on the additional ground that the information therein was input by means of a form interface does not mandate a conclusion that *all* information input by means of a form interface constitutes contents of a communication under § 2702(a). Such a conclusion would have broad implications in the civil discovery context, as information routinely obtained by subpoena no longer would be available by that means. This Court is unwilling to construe the term "contents" so broadly absent clearer direction from the Ninth Circuit or the Supreme Court.

Plaintiff further urges this Court to consider the holding in *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013). The Court does not find *Yunker* to be persuasive. First, in *Yunker* the § 2702 claim was dismissed on the ground that the plaintiff had failed to allege disclosure of contents of a communication "while in electronic storage." *Id.* at *8. That aspect of the statute is not at issue here. Second, in *Yunker* the scope of the disclosed information was broader than in the present case, including not only a universally unique device identifier and zip code, but also the user's gender and birthday. *Id.* at *6. The *Yunker* court declined to conclude that such information "cannot comprise the 'substance, purport, or meaning' of a communication." *Id.* However, the court was careful to limit its ruling to the facts before it. *Id.*

After review of the complaint and the relevant authorities, the Court concludes that the facts alleged establish that "a record or other information" about Plaintiff was disclosed to the third-party vendor rather than "contents of a communication." Given the analysis set forth herein, Plaintiff must consider whether she can allege additional facts that would demonstrate that the alleged disclosure was more than record information. Because the complaint has not previously been challenged by motion or addressed by the Court, Plaintiff is afforded the opportunity to do so. Accordingly, Defendants' motion is GRANTED with leave to amend as to Claim 4.

5. Claim 5 – Violation of California's UCL

Claim 5 asserts a violation of California Business & Professions Code § 17200 *et seq*. In order to state a claim for relief under that provision, Plaintiff must allege facts showing that Defendants engaged in an "unlawful, unfair or fraudulent business act or practice." Cal. Bus. &

Prof. Code § 17200. "Because the statute is written in the disjunctive, it is violated where a defendant's act or practice violates any of the foregoing prongs." *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1168 (9th Cir. 2012). Plaintiff asserts claims under both the unlawful and unfair prongs.[2]

While Defendants identify numerous pleading defects with respect to both prongs – for example, Plaintiff asserts a claim under the unlawful prong based upon Defendants' alleged violation of the SCA but has failed to make out a claim under the SCA – the Court concludes that the claim suffers from a more fundamental defect that obviates the need for further analysis. In order to maintain a claim under the UCL, Plaintiff must allege that she has suffered (1) economic injury (2) as a result of the alleged unfair business practice. *See Kwikset Corp. v. Sup. Ct.*, 51 Cal. 4th 310, 323 (2011). Plaintiff has not alleged any facts showing that Defendants' business practice – disclosing users' Contact Information to third-party App vendors – changed her economic position at all. Plaintiff alleges that she purchased an App for $1.77 and received that App. (Compl. ¶ 74, ECF 5-1) As is discussed in connection with the contract claim, Plaintiff has not alleged facts showing that she suffered any damages resulting from that transaction. Unless and until Plaintiff can allege economic injury resulting from Defendants' practice of disclosing Contact Information, she cannot proceed with a UCL claim.

Based upon the foregoing, the motion to dismiss is GRANTED as to Claim 5 with leave to amend.

//

//

//

//

//

[2] At the hearing, Defendants' counsel asserted that Plaintiff's UCL claim most properly should be analyzed under the fraud prong, because in essence it is a promissory fraud claim. Because Plaintiff does not expressly allege a claim under the fraud prong, the Court limits its analysis to whether Plaintiff has stated a claim under the unlawful and unfair prongs. As a practical matter, analysis under the fraud prong would not change the outcome of the motion given the Court's disposition of the claim based upon failure to allege economic injury.

IV. ORDER

(1) Defendants' Motion to Dismiss for lack of Article III standing is DENIED;

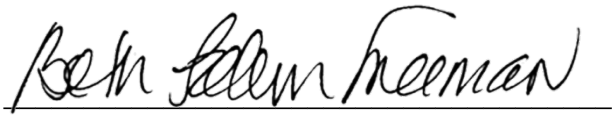
(2) Defendants' Motion to Dismiss for failure to state a claim is GRANTED as to Claims 1, 2, 4, and 5 with leave to amend and as to Claim 3 without leave to amend;

(3) Leave to amend is limited to the claims addressed in this order; Plaintiff may not add additional claims without express leave of the Court;

(3) Any amended complaint shall be filed on or before September 2, 2014; and

(4) Any amended complaint shall be electronically filed in a searchable PDF format in compliance with Civil Local Rule 5-1(e)(2).[3]

Dated: August 12, 2014



BETH LABSON FREEMAN
United States District Judge

[3] Because Plaintiff's original complaint was converted to PDF from a scanned document, the Court was unable to conduct text searches of the complaint.